PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G07C 13/00 — A1

(11) International Publication Number: WO 92/03805

(43) International Publication Date: 5 March 1992 (05.03.92)

(21) International Application Number: PCT/FI91/00261

(22) International Filing Date: 26 August 1991 (26.08.91)

(30) Priority data:
904216 27 August 1990 (27.08.90) FI

(71) Applicant: TECNOMEN OY [FI/FI]; Koronakatu 1, SF-02210 Espoo (FI).

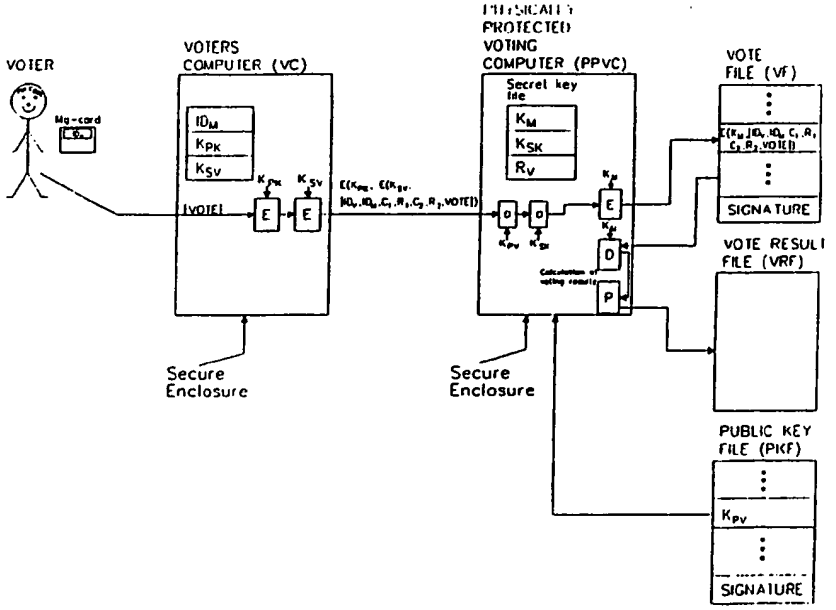
(72) Inventor: PENTTONEN, Jyrki ; Uudenmaankatu 29 C 22, SF-00120 Helsinki (FI).

(74) Agent: LEITZINGER OY; Ruoholahdenkatu 8, SF-00180 Helsinki (FI).

(81) Designated States: AT (European patent), BE (European patent), CH (European patent), DE, DE (European patent), DK, DK (European patent), ES (European patent), FR (European patent), GB, GB (European patent), GR (European patent), IT (European patent), LU (European patent), NL, NL (European patent), NO, SE, SE (European patent).

Published
With international search report.

(54) Title: METHOD FOR CONDUCTING A TELEVOTE IN A SAFE MANNER



(57) Abstract

The invention relates to a method for conducting a televote in a safe manner. All processing of voting information is effected inside a physically protected data processing unit (PPVC) in a manner that under no circumstances does any piece of voting information provided by voters appear outside the said physically protected data processing unit (PPVC) in a deciphered form or in such a form that it could be deciphered by someone else but the said physically protected data processing unit (PPVC).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MG	Madagascar
AU	Australia	FI	Finland	ML	Mali
BB	Barbados	FR	France	MN	Mongolia
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Faso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GN	Guinea	NL	Netherlands
BJ	Benin	GR	Greece	NO	Norway
BR	Brazil	HU	Hungary	PL	Poland
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	SD	Sudan
CG	Congo	KP	Democratic People's Republic of Korea	SE	Sweden
CH	Switzerland			SN	Senegal
CI	Côte d'Ivoire	KR	Republic of Korea	SU+	Soviet Union
CM	Cameroon	LI	Liechtenstein	TD	Chad
CS	Czechoslovakia	LK	Sri Lanka	TG	Togo
DE*	Germany	LU	Luxembourg	US	United States of America
DK	Denmark	MC	Monaco		

+ **Any designation of "SU" has effect in the Russian Federation. It is not yet known whether any such designation has effect in other States of the former Soviet Union.**

Method for conducting a televote in a safe manner

Televoting refers to a voting procedure, where the voters are offered the possibility of using their voting rights for example by utilizing a data communication network.

In principle, the nature of televoting is such that a data network used as a telecommunication medium must fulfil certain requirements in order to be accepted for televoting. The most important requirement is that the network must be geographically comprehensive, i.e. it must be accessible to voters as easily as possible. The telecommunication media best suitable for televoting ballots include a public dial telephone network, general circuit-switched data transmission networks or public package-switched data transmission networks.

The extensive geographical coverage of a network used as a telecommunication medium creates nevertheless a problem for conducting a vote and particularly for the preservation of a secret ballot. The fact that these networks are easily accessible makes them vulnerable in terms of privacy protection.

A traditional opinion has been that one of the major obstacles to the introduction of televoting systems has been the fact that a secret ballot cannot be guaranteed with these procedures. This invention relates to a method capable of securing secrecy in televoting ballots.

Secrecy in ballots is a sum of several different factors. The most important aspect is generally considered to be the secrecy of the voting information. This means that the choice of vote of a private voter must not under any circumstances end up in the hands of anyone else but the

voter him- or herself.

In terms of a secret ballot, another important aspect in voting systems is also the confirmation of mutual reliable identification. A system cannot be considered safe unless the voter has a positive assurance that he or she is indeed communicating with the intended voting machine and not, for example, with some eavesdropper imitating the operation of a voting machine. On the other hand, it is equally important that the voting machine has a possibility of confirming the identity of a voter. This is to make sure that the voter only has a chance to use his or her own voting right.

Another, but slightly less significant aspect in a secret ballot is generally considered the protection of the information as to whether a given voter has used his or her voting right in a given ballot. For example, this security requirement is not fulfilled in elections carried out in a traditional manner. Whether or not a given person has used his or her voting right is basically always public information.

However, in terms of a secret ballot, according to the relevant general principles, it is essential to be able to protect the information as to whether or not a voter has used his or her voting right in a given ballot. This aspect has even been the subject of rather extensive public debate. It has been stated that it is ethically wrong to compromising to reveal whether or not a voter has used his or her voting right.

A major threat to all voting systems is also such an attack on the system, which seeks to manipulate the actual outcome of an election.

THE PROCEDURE AND APPLICATIONS OF THE METHOD

A method of the invention can be applied to establish a televoting system, wherein all the above elements of a secret ballot can be secured.

Fig. 1 shows an operational block diagram for one method of this invention. It can be divided into the following elements:

1. A voter's computer (VC), whereby a person entitled to vote does the voting.

2. A physically protected voting computer (PPVC), which processes the voting data into such a form that it can be stored in a separate vote file (VF). The physically protected computer is designed in a manner that unauthorized persons have no access to recorded secret keys or other confidential information. Neither is it possible to interfere in any way with the functions, operating flow etc. carried out by the said physically protected data processing unit.

3. A vote file (VF) for storing the voting results as received from the voters. It should be appreciated that the file can be kept outside the physically protected data processing unit, but the processing thereof is nevertheless protected by means of cryptological methods. The file is protected both against disclosure (ciphering) of the data and against alteration attempts (digital signature) of the data. A seal of the file is calculated in a manner that it depends on the information bit of the file, so that the alteration of even a single bit causes approximately 50 % alteration of the seal bits.

Calculation of the seal is effected by means of a master key (K_m), which is inside the physically protected data processing unit and known only to the said voting computer (PPVC). The seal is dependent not only on the above-mentioned voting data and master key (K_m) but also on a random vector RV) created by the physically protected data processing unit itself. The purpose of this is to protect against possible attacks of copying type. These attacks involve attempts to use previously gathered sealed or ciphered information by replacing it with the present information.

4. A vote result file (VRF), wherein the voting computer (PPVC) calculates from the recorded vote file (VF) the actual outcome of a ballot.

5. A public key file (PKF) for storing a public key representing every voter.

A system of the invention can suitably be used e.g. for a continuous survey of political climate, for decisionmaking, for organizing an advisory or binding referendum for example in:

- issues concerning an entire state
- municipal affairs
- decision-making in societies and organizations (e.g. political parties)
- operations of polling firms (gallup)

A method of the invention can also be used for a number of other applications. These applications, suitable for the method, include e.g. brokerage systems for stock exchange and electronic funds transfer system.

In view of proper operation of the system, the essential feature is a physically protected voting computer (PPVC), the voter being in communication therewith by means of his or her own voter's computer (VC).

The system can also be carried out in a decentralized manner (fig. 2), e.g. a system covering the entire country can be decentralized as sub-systems in administrative districts and these, in turn, can be decentralized as sub-systems in municipalities. This produces a hierarchal system, wherein the lowest level of hierarchy, the municipalities, is provided with a required number of sub-systems consisting of voters' computers (VC) and local physically protected voting computers (LPPVC). The following level of hierarchy carries e.g. regional-level voting computers (RPPVC), in relation to which the local-level voting computers take the position of a voter. Accordingly, on the top level of hierarchy, said regional-level voting computers (RPPVC) are linked with a central physically protected voting computer (CPPVC) for calculating the national results.

Benefits gained by the method include, for example:

1. Conducting a televote even in real time while providing a secret ballot for a private voter. The real-time feature is a major benefit over traditional voting systems. Traditionally, the voters are given a possibility of influencing matters once every four years. A method of this invention is capable of providing the voting results (VRF) daily and even quicker than that.

2. Storing, protecting and sealing the voting data so as to prevent manipulation of the data.

3. Whether or not a voter has used his or her voting right can be kept secret. This is a further benefit in the method as compared to traditional voting systems.

The basic objective of the invention is to offer the voter a safe path in terms of privacy protection for carrying the voting information from a voter by way of voter's computer (VC) to voting computer (PPVC) and from there on to vote file (VF). Said vote file is a file in which the voting information or data provided by all voters is stored in a centralized manner. Another equally important objective is to supply the voters with reliable information about the voting results. This is important in order not to present the vote organizers with a possibility of manipulating the final voting results.

Achieving the above objective requires confirmation of the following aspects:

1. The voter must have a confirmation of discussing definitely with a voter's computer (VC) and not, for example, with an eavesdropper imitating the operation thereof.

2. The voter's computer (VC) must have a confirmation of the identity of a voter.

3. The voter's computer (VC) must be capable of authenticating a voting computer (PPVC), i.e. there must be mechanisms whereby the voter's computer (VC) can confirm the identity of a voting computer (PPVC).

4. The data processing and data storage performed in voting computer (PPVC) and voter's computer (VC) must

be arranged safely in terms of secrecy protection. Above all, this applies to information important in terms of secret ballot, such as the voting data of individual voters.

5. The calculation of voting results (VRF) in voting computer (PPVC) must be conducted safely. Thus, under no circumstances must voting data be allowed to leak in deciphered form outside the physically protected section of voting computer (PPVC). This means that, unless protected physically, the voting data must be provided with a protection e.g. by using cryptological methods (ciphering, sealing).

6. The algorithms to calculate vote results (VRF) must be such that counted vote results (VRF) cannot possibly be used to conclude the voting data given by an individual voter. This applies also to so-called combination attacks comprising several file searches, none of which reveals confidential information alone but a suitable combination of such file searches nevertheless does so. Thus, the vote results (VRF) calculation algorithms in voting computer (PPVC) must be provided with checks for discovering such attacks.

7. The storage of public information (e.g. public keys of public key systems) associated with ciphers and authentications being stored in voting computer (PPVC) and voter's computer (VC) must be arranged in a manner that it is not possible for outsiders to tamper with this information without voting computer (PPVC) discovering such actions.

8. There is a safe way of informing a voter of the vote results without anyone having a chance to manipulate

this information on the way.

In the realization of one method of the invention shown in fig. 1, the identification of a voter is based on a magnetic card in his or her possession and on a password known only to this particular voter.

The authentication between voting computer (PPVC) and voter's computer (VC) is effected in the present system by the application of so-called public key methods. Each voter's computer (VC) possesses its own secret key which is possessed only by said computer. This key, as well as all other confidential information in the voter's computer (VC), is retained in a physically protected location. Accordingly, the voting computer (PPVC) has its own secret key which is likewise possessed only by the said computer and is physically protected.

More detailed information about public key methods, the operating principles and reliability thereof will not be described in this context but, instead, reference is made to the items of literature listed hereinbelow.

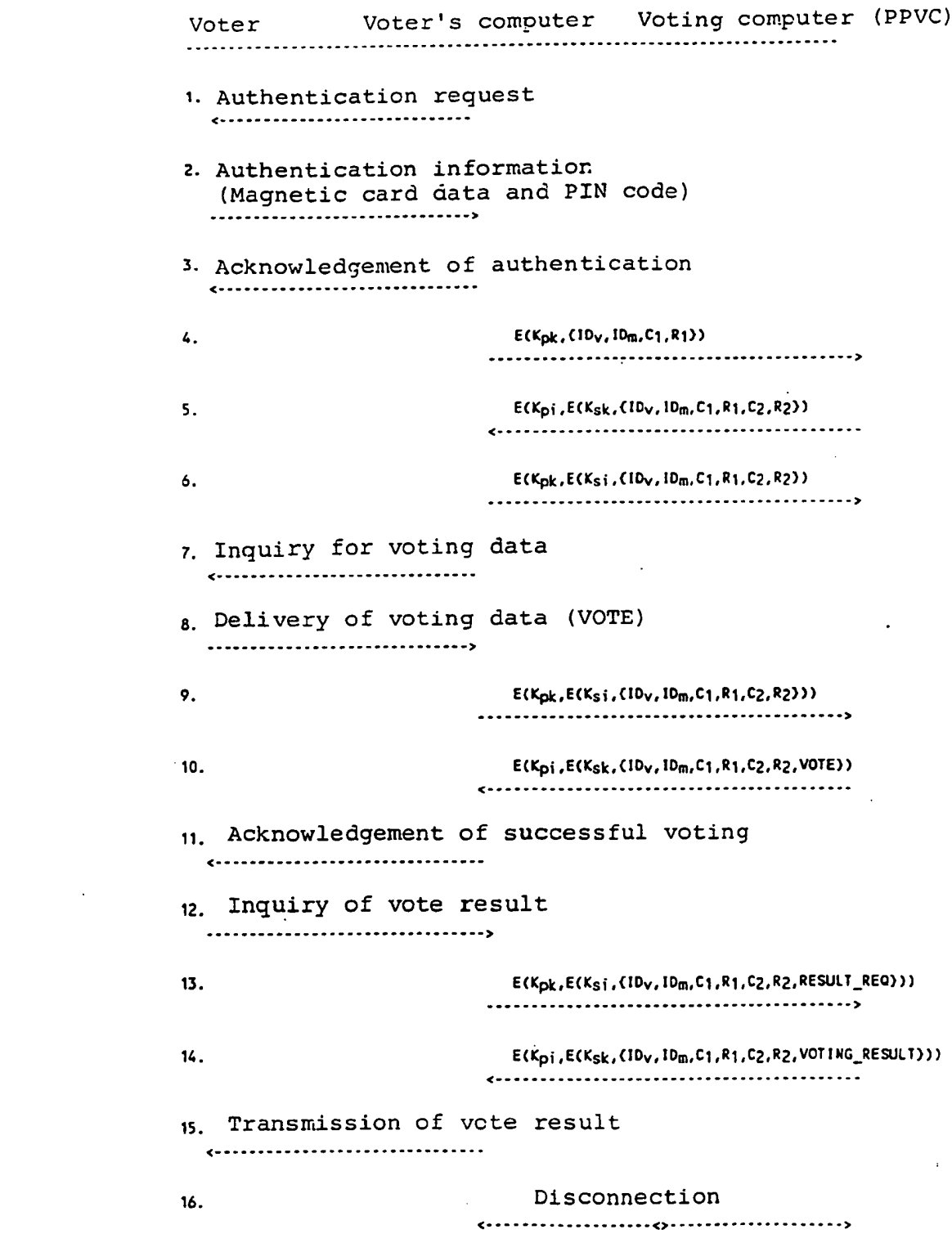
1. Baker H., Piper F., Cipher Systems, The protection of Communications, Edinburgh and London, Northwood Publications, 1982.

2. Seberry, Pieprzyk, Cryptography, An Introduction to Computer Security, New York, Prentice Hall, 1989.

3. Davies D. W., Price W. L., Security for Computer Networks, An Introduction to Data Security in Teleprocessing and Electronics Funds Transfer, Chichester, John Wiley & Sons, 1984.

EXAMPLE:

The following is a detailed description of a specific voting procedure.



The voting operation proceeds step-by-step as follows:

1. Voter's computer (VC) requests authentication.
2. Voter supplies authentication information, a PIN code and data on the tape of magnetic tape card.
3. Voter's computer (VC) checks the voter's authentication information and delivers to the voter a positive acknowledgement, in case that authentication was successful.
4. Voter's computer (VC) delivers the authentication request to voting computer (PPVC). This message is ciphered with the public key of voting computer (PPVC) and, thus, only the said voting computer (PPVC) is capable of deciphering it. This serves also as a partial authentication. If, namely, the voter's computer (VC) can make sure later that the counterpart device has been capable of correctly deciphering the message delivered thereby, the said voter's computer (VC) can confirm the identity of voting computer (PPVC). The message contains a voter's unique identification number ID_v, identification ID_m for a voter's computer, a constant field C1, and a random number R1. The reason to include constant C1 in the message is that, upon deciphering the message, the said voting computer (PPVC) can make a decision as to whether the received message is indeed the one expected to be received, in other words, intelligible. The random number is created by the voting computer (PPVC) itself and it is included in the message in order to make sure that the said authentication sequences would look different each time. This is necessary to eliminate the so-called replay attacks.
5. The voting computer (PPVC), after receiving a message

delivered by the voter's computer (VC), wherein the identity of a voter and a voter's computer is confirmed for voting computer (PPVC), checks a constant field included in the message. If the constant field is what it is supposed to be, i.e. what is agreed on a system level as an appropriate constant field, the voting computer searches a sealed public key file (PKF) for a public key matching this particular voting computer, checks the seal, and sends an authentication acknowledgement message back to the voter's computer (VC). The message contains the voter's identification ID_v, identification ID_m for voter's computer, constant C1, and random field R1 supplied by voter's computer (VC), as well as a corresponding second constant field C2 and a random field R2. The meaning of these two latter fields is the same as that of the corresponding fields supplied by the voter's computer (VC). The message is ciphered in a manner that the topmost cipher or encryption uses a public key of the voter's computer (VC) and the inner cipher or encryption uses the secret key of the voting computer (PPVC). The purpose of the topmost cipher or encryption is to prevent the disclosure of information. This is secured by the fact that no one else but the voter's computer (VC) is capable of deciphering this particular message as it requires the secret key of the voter's computer (VC), which is possessed by voter's computer (VC) only. The purpose of an inner cipher or encryption is to authenticate the voting computer (PPVC) to the voter's computer (VC). Accordingly, this is secured by the fact that it has only been possible for voting computer (PPVC) to produce the said encryption text as no one else is in possession of the said secret key. It should be noted that, after step 5, the said voting computer

(PPVC) has authenticated itself to the voter's computer (VC) but there is not yet any security as to the authenticity of a voter or voter's computer (VC), since anyone could have delivered the message mentioned in step 4.

6. The voter's computer (VC) sends out a message similar to that of the preceding step. The purpose of an outer encryption is to prevent disclosure of the information contents of the message. An encryption key used herein is the public key of the voting computer (PPVC). This encryption can only be deciphered by the voting computer (PPVC) since only that is in possession of a secret key corresponding thereto. The inner encryption is accordingly produced by using the secret key of a voter's computer, thus facilitating the authentication of the voter's computer (VC). This is because only the voter's computer (VC) has been capable of conducting the operation, it being the only one in possession of this secret key.

It should be noted that, after step 6, authentication has been performed on both sides. The voter's computer (VC) can be sure that it is communicating to the voting computer (PPVC) it is supposed to be communicating with. Likewise, the voting computer (PPVC) can be sure of the identity of the voter's computer (VC) and a voter.

7. Following step 6, with all-around authentications completed, there has also been established a safe data-transmission link between voter and voting computer (PPVC). Thus, the transmission of voting information can now be started from voter to voting

SUBSTITUTE SHEET

computer (PPVC). This is effected in two stages. Firstly, the voting computer (PPVC) requests a voter for voting information.

8. The voter replies with voting information or data of his or her choice. This data may contain quite varied information. It may contain information about a ballot to be participated in, possibly whether to cancel or alter previously given votes, whether to participate in a new ballot, and the actual voting data.

9. The voting data provided by a voter is delivered by the voter's computer (VC) to the voting computer (PPVC). The message is provided with constant and random fields similar to those included in the preceding messages. These are added for the same reason, i.e. to give the message a random nature against repetition and similar attacks. The ciphers are also produced the same way as before; the outermost cipher is again for covering the information while the innermost cipher is for the authentication of a message.

10. The voting computer (PPVC) checks the authenticity of a received message by using constant and random fields and records the voting information in a vote file. This is accompanied by checking also the integrity of a vote file by opening the seal of a vote file by using a random vector (RV) located inside the said physically protected data processing unit (PPVC) as well as a master key (K_m). The new voting information is included in the vote file by creating a new reading for the random vector (RV) and by using this and the master key (K_m) for ciphering the voting information

and for sealing it in the vote file. This is followed by delivering an acknowledgement to the voter's computer (VC). This acknowledgement is created by the application of principles similar to those included in the preceding messages to secure the secrecy of information and the authentication of a message.

11. The voting computer (PPVC) receives an acknowledgement message from the voting computer (PPVC), checks it for authenticity and, if the message has been authentic and correct, reports to a voter that the voting information delivered by him or her has now been included in the vote file. Then, the voter's computer (VC) disconnects the link.

12. A voter requests the system for vote results.

13. The voter's computer (VC) presents a voter's request for vote results to the voting computer (PPVC). This is effected by means of cipher and authentication mechanisms similar to those of the preceding steps.

14. The voting computer (PPVC) delivers a vote result calculated thereby to the voter's computer (VC). This transmission is also properly protected against possible manipulation. At this stage, secrecy of the transmitted information is no longer of utmost importance, since vote results are generally public information.

15. The voter's computer (VC) delivers the vote result information received thereby to a voter.

16. The link between voting computer (PPVC) and voter's computer (VC) is disconnected.

Claims

1. A method for conducting a televote in a safe manner, c h a r a c t e r i z e d in that all processing of voting information is effected inside a physically protected data processing unit (PPVC) in a manner that under no circumstances does any piece of the voting information delivered by individual voters appear outside the said physically protected data processing unit (PPVC) in deciphered form or in such a form that it could be deciphered by someone else but the said physically protected data processing unit (PPVC).

2. A method as set forth in claim 1, c h a r a c t e r - i z e d in that a voter's identity can be confirmed and, thus, it is secured that it is only possible for a voter to use his or her own voting right, this being secured by the fact that only a voter's computer (VC) is in possession of a secret key or some other secret information whose presence is checked by a voting computer (PPVC) and, acccrdingly, since voter's computer (VC) has identified a voter, a chain of authentication is established from the voting computer (PPVC) all the way to a voter, thus making sure of the identity of a voter.

3. A method as set forth in claim 1, c h a r a c t e r - i z e d in that a voter can confirm the authenticity of a voting computer, i.e. make sure that a voter is communicating with the particular voting computer he or she is supposed to be linked with, this being secured by the fact that only the voting computer (PPVC) is in possession of a secret key or other secret information whose presence is checked by the voter's computer (VC).

4. A method as set forth in claim 1, c h a r a c t e r -

i z e d in that the public keys of voters can be stored outside a physically protected data processing unit in a manner, however, that the keys are sealed so that the reading of the said seal depends not only on said public keys but also on a random number (RV) created by the physically protected data processing unit itself and on a fixed key (K_m), this feature making sure that it is not possible to alter the key information or e.g. to take up out-of-date information for reuse.

5. A method as set forth in claim 1, c h a r a c t e r - i z e d in that the voting information provided by voters can be stored outside a physically protected data processing unit in a manner, however, that the voting information is sealed and ciphered only with a key located inside a physically protected data processing unit so that the reading of said seal depends not only on the said voting information but also on a random number (RV) created by the physically protected data processing unit itself and on a fixed key (K_m), this feature making sure that it is not possible to alter the voting information or e.g. to take up out-of-date information for reuse.

6. A method as set forth in claim 1, c h a r a c t e r - i z e d in that vote results can be transmitted to voters in a manner that a voter can confirm the authenticity thereof, i.e. that said vote results are counted from the delivered voting information (VF) and that the vote results have not been manipulated during the count or transmission thereof.

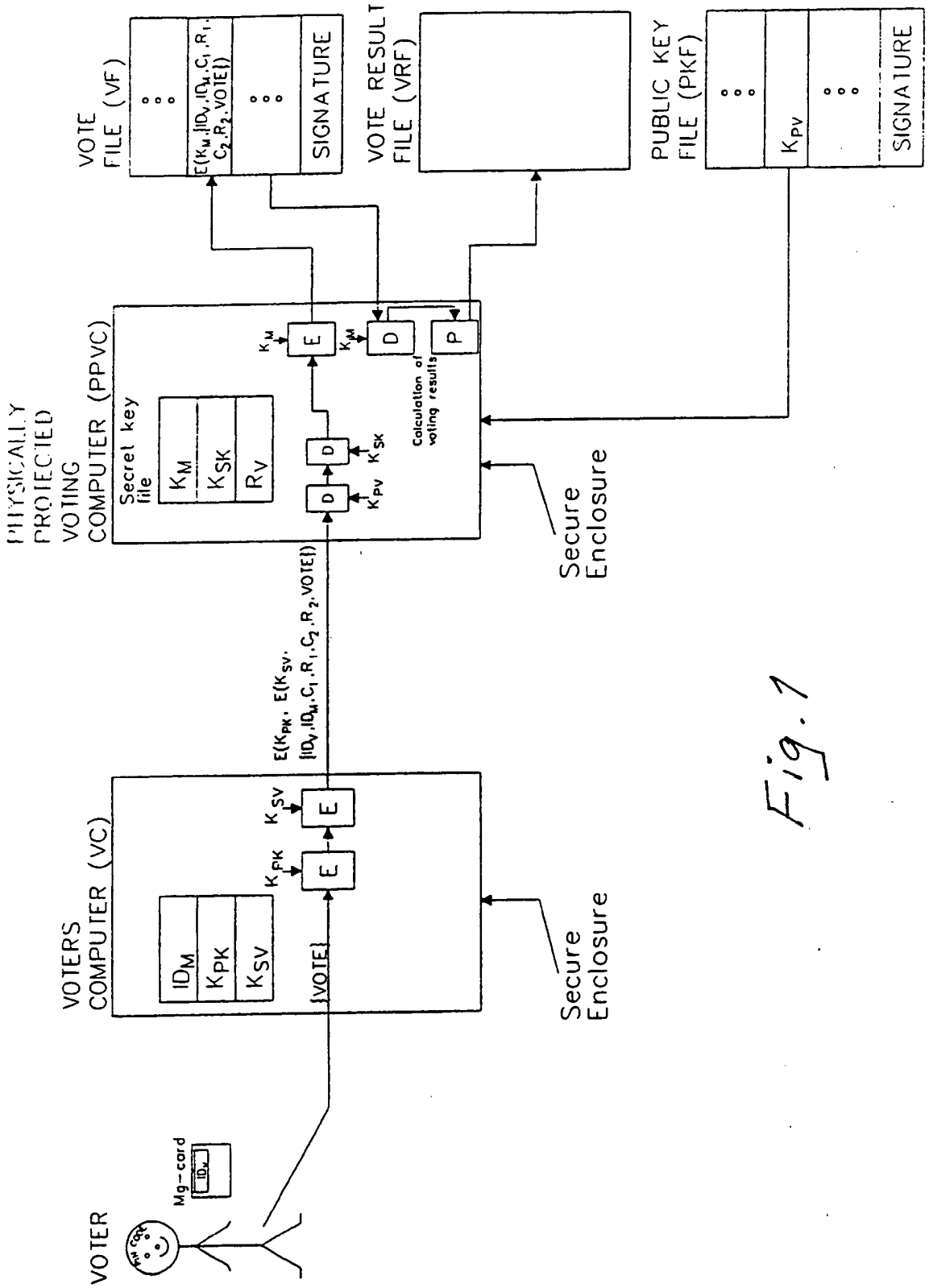
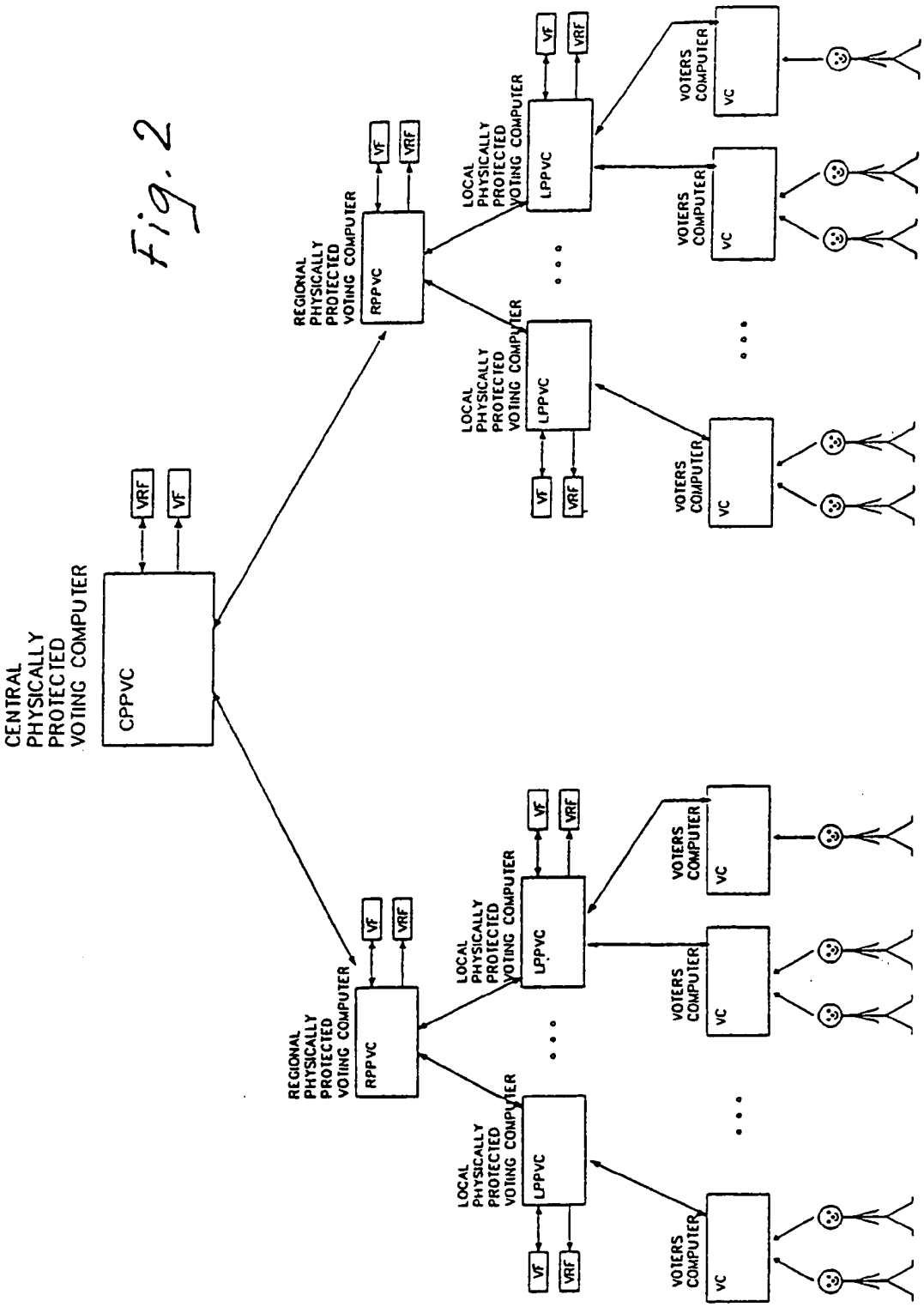

VOTE FILE (VF)
SIGNATURE
VOTE RESULT FILE (VRF)
PUBLIC KEY FILE (PKF)
SIGNATURE
PHYSICALLY PROTECTED VOTING COMPUTER (PPVC)
Secret key file
Calculation of voting results
Secure Enclosure
VOTERS COMPUTER (VC)
Secure Enclosure
VOTER
Mg-card

Fig. 1

Fig. 2


CENTRAL PHYSICALLY PROTECTED VOTING COMPUTER
CPPVC
VRF
VF
REGIONAL PHYSICALLY PROTECTED VOTING COMPUTER
RPPVC
LOCAL PHYSICALLY PROTECTED VOTING COMPUTER
LPPVC
VOTERS COMPUTER
VC

INTERNATIONAL SEARCH REPORT

International Application No PCT/FI 91/00261

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all)[6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC5: G 07 C 13/00

II. FIELDS SEARCHED

Minimum Documentation Searched[7]

Classification System	Classification Symbols
IPC5	G 07 C, G 07 F

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in Fields Searched[8]

SE,DK,FI,NO classes as above

III. DOCUMENTS CONSIDERED TO BE RELEVANT[9]

Category *	Citation of Document,[11] with indication, where appropriate, of the relevant passages[12]	Relevant to Claim No.[13]
X	SE, B, 455652 (INNOVATIONSCENTRALEN AB) 25 July 1988, see abstract; claims 1-4 --	1,2
Y		1-6
Y	SE, B, 442249 (TELEFON AB L M ERICSSON) 9 December 1985, see abstract --	1-6
A	US, A, 4290141 (R.E. ANDERSON ET AL) 15 September 1981, see the whole document --	1-6
A	EP, A1, 0420355 (N.V. NEDERLANDSCHE) 3 April 1991, see the whole document --	1-6

---

* Special categories of cited documents:[10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
12th November 1991	1991 -11- 28
International Searching Authority	**Signature of Authorized Officer**
SWEDISH PATENT OFFICE	Håkan Olsson HÅKAN OLSSON

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON INTERNATIONAL PATENT APPLICATION NO.PCT/FI 91/00261

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report.
The members are as contained in the Swedish Patent Office EDP file on 91-09-27
The Swedish Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
SE-B- 455652	88-07-25	SE-A-	8303412	84-12-16
SE-B- 442249	85-12-09	DE-A-	3469080	88-03-03
		EP-A-B-	0143096	85-05-29
		SE-A-	8306349	85-05-18
		US-A-	4629872	86-12-16
US-A- 4290141	81-09-15	NONE		
EP-A1- 0420355	91-04-03	NL-A-	8902397	91-04-16